

PRIVACY PROTECTION FOR PARTICIPATORY SENSING SYSTEM

FIELD OF THE INVENTION

[0001] Example and non-limiting embodiments of this invention relate generally to a communication network and particularly to a privacy protection technology that may be used for participatory sensing systems in the communication networks.

BACKGROUND OF THE INVENTION

[0002] Mobile phones of today have evolved from merely being phones to full-fledged computing, sensing, and communication devices. These features of mobile phones coupled with their ubiquity have paved a way for an exciting new paradigm for accomplishing large-scale sensing, i.e. participatory sensing. Participatory sensing is a concept of communities (or other groups of people) contributing sensory information to form a body of knowledge. One key idea of participatory sensing is to empower ordinary persons to collect and share sensed data from surrounding environments using their mobile devices. For example, cameras on mobile phones can be used as video and/or image sensors; embedded Global Positioning System (GPS) receivers on mobile phones can provide location information.

SUMMARY OF THE INVENTION

[0003] Example embodiments of the present invention propose an anonymous dynamic identity (ID) privacy protection method for participatory sensing with incentives. In this method, a pseudonym is used to represent a user. When a user wants to provide sensed data to a server, the user may generate a pseudonym and use the pseudonym as his or her identity. Consequently, the server and/or an adversary will not be able to track the user since the user's identity information is hidden in the whole process of communication.

[0004] An aspect of the invention relates to a method. The method comprises: generating a pseudonym, at a user equipment, in association with sensed data; calculating a unique value based upon the pseudonym using a first algorithm; sending the unique value and the sensed data to a server; receiving a certificate from the server, wherein the certificate is calculated based at least in part on the unique value using a second algorithm; and sending at least the pseudonym and the certificate to a certification center via a secure channel, for obtaining a reward associated with the sensed data, wherein the certification center is internal or external to the server.

[0005] A second aspect of the invention relates to another method. The method comprises: receiving, at a server, a unique value and sensed data from a user equipment, wherein the unique value is calculated at the user equipment using a first algorithm based upon a pseudonym generated by the user equipment; calculating a certificate based at least in part on the unique value using a second algorithm; and sending the certificate to the user equipment so that the certificate may be forwarded to a certification center for obtaining a reward associated with the sensed data, wherein the certification center is internal or external to the server.

[0006] A third aspect of the invention also relates to a method. The method comprises: receiving, at a certification center, at least a pseudonym and a certificate via a secure channel from a user equipment; calculating a unique value using a first algorithm based upon the pseudonym; calculat-

ing at least one reference value based at least in part on the unique value using a second algorithm; comparing the at least one reference value with the received certificate; and if the at least one reference value matches the received certificate, confirming validity of the received certificate so that the user equipment may obtain a reward associated with sensed data; wherein the certification center is internal or external to a server.

[0007] A fourth aspect of the invention relates to an apparatus. The apparatus comprises: a sensor arrangement comprising at least one sensor for sensing data; at least one processor; and at least one memory including a computer program code, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the apparatus to: generate a pseudonym in association with sensed data; calculate a unique value based upon the pseudonym using a first algorithm; send the unique value and the sensed data to a server; receive from the server a certificate, wherein the certificate is calculated at the server based at least in part on the unique value using a second algorithm; and send at least the pseudonym and the certificate to a certification center via a secure channel, for obtaining a reward associated with the sensed data, wherein the certification center is internal or external to the server.

[0008] A fifth aspect of the invention relates to another apparatus. The apparatus comprises: at least one processor; and at least one memory including a computer program code, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the apparatus to: receive a unique value and sensed data from a user equipment, wherein the unique value is calculated at the user equipment using a first algorithm based upon a pseudonym generated by the user equipment; calculate a certificate based at least in part on the unique value using a second algorithm; and send the certificate to the user equipment so that the certificate may be forwarded to a certification center for obtaining a reward associated with the sensed data, wherein the certification center is internal or external to the apparatus.

[0009] A sixth aspect of the invention also relates to an apparatus. The apparatus comprises: at least one processor; and at least one memory including a computer program code, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the apparatus to: receive at least a pseudonym and a certificate via a secure channel from a user equipment; calculate a unique value using a first algorithm based upon the pseudonym; calculate at least one reference value based at least in part on the unique value using a second algorithm; compare the at least one reference value with the received certificate; and if the at least one reference value matches the received certificate, confirm validity of the received certificate so that the user equipment may obtain a reward associated with sensed data; wherein the apparatus is internal or external to a server.

[0010] A seventh aspect of the invention relates to a method, wherein an encryption function is used to calculate a certificate which is used for obtaining a reward by a user.

[0011] Further, the proposed method uses a one-way hash function to convert the user's pseudonym into a unique value. The value transmitted between the user and the server is the unique value and the one-way hash function is irreversible, so the adversary is not possible to obtain the user's pseudonym.